ELEN E6883: Introduction to Blockchain Technology

Homework 1

Tong Wu, tw2906

Problem 1

Section 1

Three properties that a Cryptographic Hash Function needs to satisfy is: preimage resistant, collision resistant and second preimage resistant.

- Preimage resistant

  For the cryptographic hash function:

  $$y = h(x)$$

  Given the output y of n bits, finding preimages x such that $y = h(x)$ requires $\mathrm{O}(2^n)$ time. It should be hard to find a message x with a given hash value y.

- Collision resistant

  For the hash function $h(x)$, it is infeasible to find two distinct values x and x' such that:

  $$h(x) = h(x')$$

- Second preimage resistant

  Given one message x it should be hard to find another message x' such that:

  $$h(x) = h(x')$$

  Given an output of n bits and a message x, it requires $\mathrm{O}(2^n)$ time before one can find a second preimage x'.

Section 2

The has value of the message should be encrypted with a user's private key rather than the public key. So the answer is false.

Section 3

RSA, Elliptic Curve.

Section 4

True

Problem 2

Theorem:

Let $r_1, r_2, \dots r_n \in 1, 2, \dots, N$ be independent, identically distributed integers, then:

$$Pr[r_i = r_j | i \neq j] \geq \frac{1}{2} \text{ for } n = 1.2 \times \sqrt{N}$$

Proof:

$$\begin{aligned} Pr[r_i = r_j | i \neq j] &= 1 - Pr(r_i \neq r_j | i \neq j) \\ &= 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{N}) \end{aligned}$$

According to Bernoulli's inequality $e^x \geq 1 + x$:

$$\begin{aligned} &\geq 1 - \prod_{i=1}^{n-1} exp(-\frac{i}{N}) \\ &= 1 - exp(-\sum_{i=1}^{n-1} \frac{i}{N}) \\ &= 1 - exp(-\frac{1}{N}\frac{n^2 - n}{2}) \\ &\approx 1 - exp(-\frac{1}{N}\frac{n^2}{2}) \end{aligned}$$

Then for $n = 1.2 \times \sqrt{N}$:

$$\begin{aligned} &= 1 - exp(-0.72) \\ &\geq \frac{1}{2} \end{aligned}$$

Problem 3

Section 1

The attacker cannot steal funds from the input address of the transaction submitted to the Bitcoin network if the private key is used to sign the entire transaction. Because the private key not only contains the private key information, but also encrypts the transaction together with the private key into the signature. In this way, even if the

attacker obtains the signature, the attacker cannot decrypt the private key or modify the transaction information or steal funds.

Section 2

The attacker can steal funds from the input address of the transaction submitted to the Bitcoin network if the private key is used to sign the output of the transaction but nothing else. Because the signature must include the entire transaction, not just the output, to prove that the user has the ownership of the funds and that the transaction has not been tampered with. The attacker can copy the transaction and change the ID of the transaction in order to done an unauthorized transaction from user.

Problem 4

Section 1

According to the longest chain rule, it can not be confirmed that which chain is going to be the longest chain confirmed after n-1 blocks created after this block on the main chain.

Section 2

Because the seller is facing the double spending issue, such as Finney attack by a malicious miner. The buyer can includes a transaction sending some coins to himself in his mined block, then the buyer can withholds the mined block and instead send the same coins to a merchant. Once he finds the block and he will broadcasts the block when the merchant accepts the payment and irreversibly provides the service.

Problem 5

Section 1

$$TPS = \frac{1M}{250} / (10 \times 60) \approx 6.6667$$

Section 2

Increasing the block size:

By increasing the block size, more transactions can be stored in a single block, which increases the TPS. However, increasing the block size also increases the size of the blockchain, which can cause that larger blocks can take longer to propagate through the network, which can slow down the overall performance of the blockchain. Also, the probability of forking increases, which will obstruct in increasing the TPS.

Shortening the block generation interval:

By shortening the block generation interval, more blocks can be generated in a given time, which also increases the TPS. However, shortening the block generation interval also increases the difficulty of mining blocks and the proof-of-work difficulty, which can result in centralization of the network. Also, the probability of forking increases, which will obstruct in increasing the TPS.